ITACS

Information Technology and Communications Services

Naval Postgraduate School, Monterey, California

NPS ITACS Policy

Category: 900 – Client System Support

ITACS Policy: 902 – Local Administrator privileges on a Windows workstation

Approval: ITACS and the IT Task Force

Timeline: Date Published: 1 May 2001
Revision date: 1 June 2006
Effective date: 1 June 2006

Definitions: This policy is applicable to all Students, Faculty and Staff of the Naval Postgraduate School.

The term “typical end-user” refers to a computer end-user that expects the system level configuration of their computer to be maintained by a member of the IT technical support staff. Typical end-users envision their computer as a business tool and do not want to be concerned with the details required to keep the computer functional.

The term “local administrator” refers to a special, privileged end-user that has inherent operating system configuration rights and capabilities not available to a typical end-user. Local administrators have rights to change system-level parameters.

Local administrator privileges are normally reserved for the ITACS system administrators (staff) or for an expert end-user.

Policy: If a typical end-user chooses to be granted local administrator privileges, then system-level functionality for their computer will become the responsibility of that end-user. If the system fails, ITACS technical support service will be limited to the recovery of the system by the re-installation of the generic baseline software (O/S and standard applications) that was configured for that particular computer when it was originally placed into service.

It is the responsibility of the end-user having local administrative privileges to reinstall the local applications and recover the associated data files.

Guidelines: An end-user that is granted local administrator privileges becomes responsible for the configuration of their computer. ITACS will provide support for the standard applications and required operating system and anti-virus patches via remote tools.

Application software licensing, and product upgrading/patching, for end-user installed applications is the responsibility of that end-user.

ITACS recovery of a damaged software environment is limited to the re-installation of the standard baseline image (applications and configuration) for that computer.

The end-user agrees:

1. To maintain a separate local administrative account on the system. Specifically, the "typical end-user" level account used for email and web browsing will not be added to the local administrative group. All local administrative account passwords will meet the DoD strong password criteria.
2. To not change the network adapter configuration.
3. To not change the name of the computer.
4. To not change the Landesk account created on the computer for remote management.

End- users that require local administrator privileges will complete the attached request and forward to the Technology Assistance Center for processing.

Request for Workstation Local Administrator Privilege

____

Name (print) Date

I agree to the Guidelines contained in ITACS policy 902

____

Signature

Computer(s) for which local administrator privilege is requested:

____

Computer name(s)